Fintechs: uniquely exposed

What is the right approach to risk management for uniquely exposed fintechs?

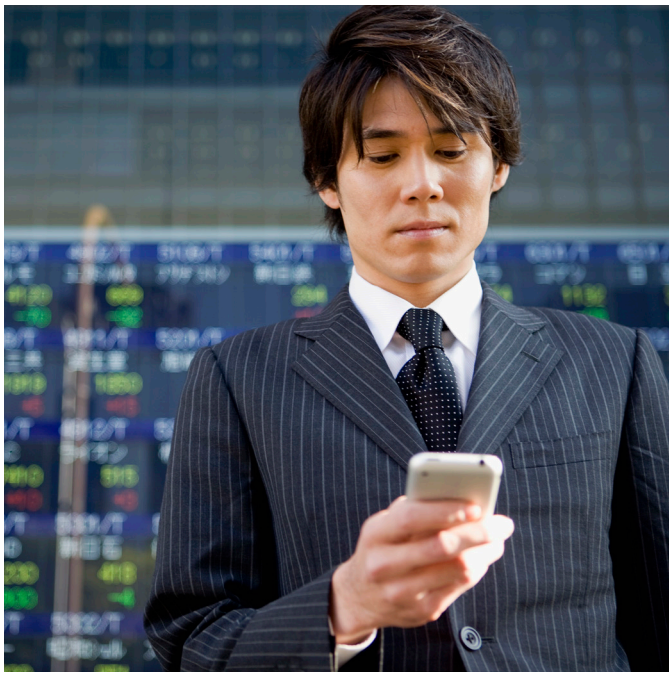
Fintech and payment services organisations have special needs when it comes to risk management and insurance strategies. Solutions need to be carefully analysed and evaluated.

There is significant innovation and disruption occurring across the financial products and services landscape where fintechs (non-bank financial technology businesses) increasingly offer services that leverage, integrate and directly compete with banks and established lenders.

The rapid evolution and expansion of fintech offerings is particularly noticeable in payment services, which includes payment processors, pay advance services and fintech lending. Many payment services organisations have experienced accelerated growth in the past two years, increasingly expansive client demands and the need to build risk management and risk registers, compliance, and insurance processes within their business.

Fintechs that offer payment/lending services are also the focus of regulators, with greater scrutiny in relation to how they manage consumer data, compliance with payment and financial services laws, transparency across their service offering, and demonstratable processes to protect consumers and vulnerable stakeholders.

As money and other financial instruments (such as cryptocurrency and digital currencies) become an increasing component of fintech service offerings, these organisations are also becoming subject to increasingly complex technology focused, financial and credit regulations including obligations under the Corporations Act 2001 (Cth), National Customer Consumer Protection Act 2009 (Cth), Payment Systems (Regulation) Act 1998 (Cth) and ASIC Act 2001 (Cth). The environment is made more challenging by the need for fintechs to carefully navigate Anti-Money Laundering Laws and Counter-Terrorism Financing (AML/CTF) obligations. Further, where fintech payment services are provided to individuals or SMEs, such as in the form of P2P lending or retail offerings, they are captured by Australian consumer law guarantees, implied warranties, and unfair contractual terms.



Diverse risk challenges

Fintechs have diverse and multi layered risk challenges that require them to adopt a strong risk management approach; the most effective way of doing so is to focus on the key classes of risk that impacting them and examine how these exposures impact their goals and priorities. Many risk classes for fintech firms are consistent with traditional organisations but several unique exposures are commonly overlooked.

One such issue, is that many fintech organisations are underpinned by industry partnerships and depend upon integrating numerous third party technologies into the service offering delivered to customers. This creates added risks across IT development processes, client engagement and managing third party contractual relationships. Assessing and mitigating risks across these topics can require broad cross-functional knowledge covering legal risks, governance, technology, business strategy, insurance, and the wider commercial market. It is critical that fintech firms examine these matters collectively as part of their risk management processes, to avoid unintentional exposure.

Another difficulty for fintechs is that customers often view them as providers of "turnkey" end-to-end solutions. Tied to this is an expectation that the fintech provider's solution can be easily implemented, and support each customer's key business processes based on tailored solutions. Fintech firms often take on significant responsibility for services availability and responsibilities for the successful delivery for a client's required outcome, including day to day maintenance/troubleshooting, updating of any software and training for client staff. Because substantive performance and support demands are placed on fintechs there can also be difficulty identifying where the boundaries of service provider accountability reside, and how client and third-party stakeholder complaints should be effectively triaged and managed.

As well as facing broad regulatory obligations, there are also growing demands for fintech firms to adopt a code of practice that encourages transparency and ethical behaviour. Increasingly, these requirements are also being tied to privacy behaviours and artificial intelligence concerns around cohesiveness, consent, and derivative data usage. Industry standards have not been adopted across all fintech bodies other than ASIC's recommendations for certain sectors, such as Buy-Now-Pay-Later institutions, to develop their own governing bodies for self-regulation.

From a privacy perspective, key obligations are imposed under the Privacy Act 1988 (Cth) and Corporations Act 2001 (Cth). Consumer data rules and emerging laws for critical infrastructure and ransomware reporting are also a growing area of concern, especially where fintechs take on considerable amounts of consumer data to generate insights into individuals' habits and engage in fraud detection to reduce AML/CTF exposures. ASIC has also highlighted that privacy and data security is a key component of a financial service providers' risk management systems. The role fintechs commonly plays as third-party data aggregators and information processors can also create further data governance risks.

Separately for fintechs and especially for start-ups, laws around intellectual property rights and registration boards may not be properly considered. In such a niche space, overlapping ideas are rife and potential lengthy litigations over breaches of intellectual property rights are of concern. It is very important that organisations are aware of new patent applications to ensure they are not improperly using registered IP.

Fintech organisations that fail to effectively manage the personal and financial information of their consumer base may also face significant notification and incident remediation requirements, contractual liabilities and long-term reputational harm.

Insurance – getting maximum cost benefit

Effective fintech insurance programs should respond to the scope and breadth of identified key risks, and the organisation's overall compliance burden. Many of the insurance products fintechs typically purchase are subject to hardened market conditions and high premium costs. For these reasons, insurance limits and policy structures should be carefully analysed to provide maximum cost benefit.

Where fintechs hold an Australian Financial Services Licence (AFSL), additional insurance requirements will arise – part of the organisation's obligations to have in place adequate arrangements for compensating clients for losses suffered, and enough resources to provide the financial services covered by the license. Similar issues also arise where organisations hold an Australian Credit Licence.

The key components of a fintech's insurance program will include:

- Professional Indemnity (PI) – coverage for breaches of professional services
- Directors & Officers (D&O) Liability
- First party crime and fidelity cover
- Dedicated Cyber Liability insurance
- Public and Products Liability
- Statutory Liability

In some cases, fintechs will pursue packaged underwriting products which provide multiple covers combined into a single wording. While some of these wordings can be effective, they should be carefully analysed as many packaged solutions contain smaller insurance limits and significantly pared back levels of coverage. Some packaged solutions are also sold as a "one size fits all" with little consideration for significant coverage gaps, which can result in the organisation's insurance program not being fit for purpose and unresponsive to their needs.

Further consideration should also be given to situations where fintechs operate as an authorised representative under another organisation's AFSL. In some cases, authorised representatives can be covered as an insured within the licensee's insurance programs, however many carriers impose restrictive conditions and insurers will take a dim view of any authorised representatives whose services go beyond the key activities of the licensee.

Contractual relationships entered into by fintechs also often impose insurance program requirements. We have seen a growing trend of fintechs being required to hold higher levels of PI coverage, as well as specific cyber insurance coverages. As fintechs gain scale and deal with larger enterprise clients, counterparty insurance demands will also grow and impose additional jurisdiction criteria and prescribed coverages. In the current market, limited insurers are comfortable in providing any levels of cover for fintechs who are exposed to offshore legal requirements.

Exclusions commonly seen on traditional policies can also create unique challenges for fintech firms. Cyber exclusions that sit within D&O and PI wordings can pose real risk to a fintech organisation, given that service availability failures and data loss events can create significant third party liability, and financial services exclusions on PI policies can similarly cause issues, given the overlap between technology and financial service offerings. Coverages for business interruption and crime must also be matched to the organisation's circumstances and the key scenarios likely to create loss. Ultimately the ability to tailor and analyse cover is central to fintechs in establishing confidence in their insurance arrangements.

Get the right support

In the current environment, fintech providers must partner with risk and insurance experts who understand their business and have the technical excellence to deliver insurance outcomes.

WTW has invested in specialist technology risk experts who have successfully delivered risk transfer solutions and supported wider risk management initiatives that mitigate and prevent underlying risk.

We also proactively partner with clients to develop proposal and market materials and have a track record of providing cost effective and creative outcomes to meet our clients' individual needs. If you require assistance or further information on any of the issues outlined in this article do not hesitate to reach out to our team.

Contact WTW

For any further information, please contact:

Benjamin Di Marco
Cyber and Technology Risk Specialist – FINEX Australasia
M: +61 478 312 988
benjamin.dimarco@willistowerswatson.com

Anthony Kumar
Lead Associate, Cyber and Technology – FINEX Australasia
M: +61 478 307 113
anthony.kumar@willistowerswatson.com

About WTW

Willis Australia Limited | ABN 90 000 321 237 | AFSL No. 240600
CKA Risk Solutions Pty Ltd | ABN 33 109 033 123 | AFSL No. 276915

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organisational resilience, motivate your workforce and maximise performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

WTW833AU

wtwco.com.au